H

UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/513,065	02/24/2000	Chi-Pei Michael Hsing	ST9-99-167	5699

7590 11/24/2003

SUGHRUE, MION, ZINN, MACPEAK & SEAS, PLLC
2100 Pennsylvania Avenue, N.W.
Washington, DC 20037-3213

EXAMINER	
KIM, JUNG W	

ART UNIT	PAPER NUMBER
2132	6

DATE MAILED: 11/24/2003

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No.	Applicant(s)	
	09/513,065	HSING ET AL.	
	Examiner	Art Unit	
	Jung W Kim	2132	

-- The MAILING DATE of this communication appears on the cover sheet with th correspond nce address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133).
- Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☐ Responsive to communication(s) filed on _____ .

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) 1-36 is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) 1-36 is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☒ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on 24 February 2003 is/are: a)☒ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

11)☐ The proposed drawing correction filed on _____ is: a)☐ approved b)☐ disapproved by the Examiner.

If approved, corrected drawings are required in reply to this Office action.

12)☐ The oath or declaration is objected to by the Examiner.

Priority under 35 U.S.C. §§ 119 and 120

13)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____ .

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

14)☐ Acknowledgment is made of a claim for domestic priority under 35 U.S.C. § 119(e) (to a provisional application).

a) ☐ The translation of the foreign language provisional application has been received.

15)☐ Acknowledgment is made of a claim for domestic priority under 35 U.S.C. §§ 120 and/or 121.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☒ Information Disclosure Statement(s) (PTO-1449) Paper No(s) 2,5 .
4) ☐ Interview Summary (PTO-413) Paper No(s). _____ .
5) ☐ Notice of Informal Patent Application (PTO-152)
6) ☐ Other: .

DETAILED ACTION

Specification

1. The title of the invention is not descriptive. A new title is required that is clearly indicative of the invention to which the claims are directed. The following title is suggested: 'Secure access to a unified logon-enabled data store using credentials'.

Claim Rejections - 35 USC § 103

2. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

3. Claims 1-12 are rejected under 35 U.S.C. 103(a) as being unpatentable over Stallings Cryptography and Network Security 2nd Edition (hereinafter Stallings) in view of Lai et al. "User Authentication and Authorization in the Java Platform" (hereinafter Lai). The user authentication method, as disclosed in the applicant's claims, reads into basic trusted third part authentication methodologies using encrypted credentials or certificates for user verification, which is provided by the third party. Kerberos, an authentication service developed as part of the Athena project at MIT, is one of the better-known and implemented services that follow this authentication format. The features of Kerberos are more comprehensive then the invention claimed by the applicant, but, in spirit, the applicant's invention follows the same procedure to authenticate a user to a service. Stallings predicates the disclosure of the Kerberos

authentication service with a description of a simple authentication procedure to provide an overview of the general structure of Kerberos. This simple authentication dialogue substantially covers the claimed invention.

4. As per claim 1, Stallings discloses a simple authentication dialogue that uses a central authentication server to log a client onto a network of distributed services (see Stallings, page 326, 'A Simple Authentication Dialogue'). This simple authentication dialogue uses a centralized server to securely identify users by obtaining information from the user and then sending a ticket back to the user, which comprises of an encrypted message containing the identification of the client, the network address of the client, and the identifier of the service. This generated ticket, in addition to an identifier of the client, is sent to the service, whereupon, the service decrypts the ticket and compares the identification with the parsed identification. Since only the authentication server and the service share the private encrypted key, only the authentication server could have encrypted the ticket when issued to the client. Hence, if the parsed id matches the id sent by the client, then the request is accepted (see Stallings, page 326, steps 1, 2, and 3). Stallings is silent on the matter of supplying both a username and a computer identifier to authenticate a parsed username and parsed computer identifier. However, at the time the applicant's invention was made, because of the increasingly distributed nature of computing services, it became evident in the art that user identification needed to be based on two parts: a unique name for the user and an address (or computer id) of the user's terminal. Lai discloses the need for this type of

access identification in a networked computer system since users have a plurality of access points to a single service (see Lai, Section 5, 'Authorization'). Furthermore, in a secure computing system, where a user has been authorized and the physical terminals from where the user accesses the services are deemed secure, authentication of a user session only needs to verify that a server request from a user specifies who they say they are and where they are accessing the service. Therefore, it would be obvious to one of ordinary skill in the art at the time the invention was made, for the identity of a user during a session to comprise a username and a computer identification as taught in Lai in the simple authentication dialogue as taught by Stallings. Motivation for such an implementation would enable the invention to prevent identity duplicity by ascertaining a user by a unique name and a computer identifier. As such, the invention covered by Stallings comprises the following steps of:

a) receiving an authentication key, a user name, and a computer identifier;

b) parsing the authentication key to obtain a parsed user name and computer identifier;

c) validating the received user name and computer identifier using the parsed user name and computer identifier (see Stallings, page 326, steps 1-3 as modified by Lai, Section 5, 'Authorization').

The aforementioned covers claim 1.

5. As per claim 2, Stallings covers a method of providing security for a computer connected to a data store as outlined above in the claim 1 rejection under 35 U.S.C.

103(a). In addition, the validating step comprises determining whether the received user name and computer identifier match the parsed user name and computer identifier (see Stallings, page 326, step 3; final paragraph).

6. As per claim 3, Stallings covers a method of providing security for a computer connected to a data store as outlined above in the claim 2 rejection under 35 U.S.C. 103(a). In addition, a match indicates that the received user name and computer identifier are valid (see Stallings, page 326, step 3; constitution of 'Ticket'; final paragraph).

7. As per claim 4, Stallings covers a method of providing security for a computer connected to a data store as outlined above in the claim 1 rejection under 35 U.S.C. 103(a). In addition, the method further comprises, before parsing, decrypting the authentication key (see Stallings, page 326, final paragraph).

8. As per claims 5 and 6, Stallings covers a method of providing security for a computer connected to a data store as outlined above in the claim 1 rejection under 35 U.S.C. 103(a). In this method, as disclosed above, the authentication server and the service share a secret key. An authentication key encrypted with the secret key could only be encrypted by the authentication server, and hence, the service accepts the user once the authentication key is decrypted and the parsed username and parsed computer identification matches the username and computer identification sent from the

user (see Stallings, page 326, third paragraph as modified by Lai, Section 5, 'Authorization'). Stallings is silent on the matter of obtaining a server user identifier and password to authenticate the user into the service. However, the step of providing a server user identifier and corresponding password is an obvious feature. Services typically provide different types of services based on the user of the service. As an example, Lai discloses the implementation of roles in a JAAS authentication architecture. Role assignment affords certain privileges to certain users (see Lai, Section 5.1, Figures 5, 6, and 7), and by assigning a service user identifier and corresponding password, the service can match a role with the user. Furthermore, by separating the server user identification from the authentication procedure to establish the unified login-id of the user, the two portions become decoupled, which can allow for easier integration of the authentication server with the services. Therefore, it would be obvious to one of ordinary skill in the art at the time the invention was made to include a server user identifier and the corresponding server user password in the authentication key then use this pair to establish a session at the service once the user's username and computer id has been verified to be the same as the parsed username and parsed computer id. Motivation for such an implementation would provide a simple and modular means of allocating a type of service to the user once the user has been verified. The aforementioned covers claims 5 and 6.

9. As per claim 7, Stallings covers a method of providing security for a computer connected to a data store as outlined above in the claim 6 rejection under 35 U.S.C.

103(a). In addition, multiple users share one server user identifier and server password (see Lai, Section 5.1, Figures 6 and 7).

10. As per claim 8, Stallings covers a method of providing security for a computer connected to a data store as outlined above in the claim 1 rejection under 35 U.S.C. 103(a). In addition, the method further comprises generating the authentication key (see Stallings, page 326, third paragraph; step 2).

11. As per claim 9, it is a method claim corresponding to claims 6 and 8 and it does not teach or define above the information claimed in claims 6 and 8. Therefore, claim 9 is rejected under Stallings in view of Lai for the same reasons set forth in the rejections of claims 6 and 8.

12. As per claim 10, Stallings covers a method of providing security for a computer connected to a data store as outlined above in the claim 8 rejection under 35 U.S.C. 103(a). In addition, the method further comprises encrypting the authentication key (see Stallings, page 326, third paragraph; step 2).

13. As per claim 11, Stallings covers a method of providing security for a computer connected to a data store as outlined above in the claim 8 rejection under 35 U.S.C. 103(a). In addition, the method further comprises forwarding the authentication key to a user (see Stallings, page 326, third paragraph; step 2).

14. As per claim 12, it is a method claim corresponding to claims 1-11 and it does not teach or define above the information claimed in claims 1-11. Therefore, claim 12 is rejected under Stallings in view of Lai for the same reasons set forth in the rejections of claims 1-11.

15. As per claims 13-24, they are apparatus claims corresponding to claims 1-12 and they do not teach or define above the information claimed in claims 1-12. Therefore, claims 13-24 are rejected under Stallings in view of Lai for the same reasons set forth in the rejections of claims 1-12.

16. As per claims 25-36, they are article of manufacture claims corresponding to claims 1-12 and they do not teach or define above the information claimed in claims 1-12. Therefore, claims 36-25 are rejected under Stallings in view of Lai for the same reasons set forth in the rejections of claims 1-12.

Conclusion

The prior art made of record and not relied upon is considered pertinent to applicant's disclosure.

Kung U.S. Patent No. 5,241,594 discloses a one-time logon means and methods for distributed computing systems.

Blakley,III et al. U.S. Patent No. 5,604,490 discloses a method and system for providing a user access to multiple secured subsystems.

Sadovsky U.S. Patent No. 5,689,638 discloses a method for providing access to independent network resources by establishing connection using an application programming interface function call without prompting the user for authentication data.

Wu et al. U.S. Patent No. 5,774,551 discloses a pluggable account management interface with unified login and logout and multiple user authentication services.

Fortinsky U.S. Patent No. 5,815,574 discloses a provision of secure access to external resources from a distributed computing environment.

Cohen et al. U.S. Patent No. 6,178,511 discloses a coordinating user target logons in a single sign-on environment.

Shannon U.S. Patent No. 6,233,618 discloses an method for access control of networked data.

Fang et al. U.S. Patent No. 6,243,816 discloses a single sign-on mechanism personal key manager.

Jin et al. U.S. Patent No. 6,311,275 discloses a method for providing single step log-on access to a differentiated computer network.

Cole et al. U.S. Patent No. 6,359,711 discloses a system and method for supporting a worker in a distributed work environment.

Stoltz et al. U.S. Patent No. 6,615,264 discloses a method and apparatus for remotely administered authentication and access control.

Bryant "Designing an Authentication System: a Dialogue in Four Scenes".

Steiner et al. 'Kerberos : An Authentication Service for Open Network Systems'.

Kohl et al. 'The Evolution of the Kerberos Authentication Service'.

Samar et al. 'Making Login Services Independent of Authentication Technologies'.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Jung W Kim whose telephone number is (703) 305-8289. The examiner can normally be reached on M-F 9:00 A.M. to 5:00 P.M..

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Gilberto Barron can be reached on (703) 305-1830. The fax phone number for the organization where this application or proceeding is assigned is (703) 872-9306.

Any inquiry of a general nature or relating to the status of this application or proceeding should be directed to the receptionist whose telephone number is (703) 305-3900.

Jung W Kim
Examiner
Art Unit 2132

Jk
November 10, 2003

AYAZ SHEIKH
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100